Glossary

BGP: Border Gateway Protocol is primarily used to connect the networks of large organizations that have two or more ISP connections, or between other autonomous systems. If used in such a situation, a FortiGate can use BGP for routing.

Certificates: In networking, certificates (including public key certificates, digital certificates, and identity certificates) provide digital signatures for websites or other electronic communication and allow you to verify whether a digital identity is legitimate.. A FortiGate can use certificates for many things, including SSL inspection and user authentication.

CLI: The Command Line Interface is a text-based interface used to configure a FortiGate unit. Most steps in the FortiGate Cookbook use the Graphical User Interface (see GUI), but some configuration options are only available using the CLI.

DHCP: Dynamic Host Configuration Protocol is a networking protocol that allows devices to request network parameters, such as IP addresses, automatically from a DHCP server, reducing the need to assign these settings manually. A FortiGate can function as a DHCP server for your network and can also receive its own network parameters from an external DHCP server.

DMZ: A Demilitarized Zone is an interface on a FortiGate unit that provides external users with secure access to a protected subnet on the internal network without giving them access to other parts of the network. This is most commonly done for subnets containing web servers, which must be accessible from the Internet. The DMZ interface will only allow traffic that has been explicitly allowed in the FortiGate's configuration. FortiGate models that do not have a DMZ interface can use other interfaces for this purpose.

DNS: Domain Name System is used by devices connecting to the Internet to locate websites by mapping a domain name to a website's IP address. For example, a DNS server maps the domain name www.fortinet.com to the IP address 66.171.121.34. Your FortiGate unit controls which DNS servers the network uses. A FortiGate can also function as a DNS server.

ECMP: Equal Cost Multipath Routing allows next-hop packet forwarding to a single destination to occur over multiple best paths that have the same value in routing metric calculations. ECMP is used by a FortiGate for a variety of purposes, including load balancing.

Explicit Proxy: Explicit proxy is a type of configuration where all clients are configured to allow requests to go through a proxy server, which is a server used as an intermediary for requests from clients seeking resources from other servers. When a FortiGate uses explicit proxy, the clients sending traffic are given the IP address and port number of the proxy server.

FortiAP: A FortiAP unit is a wireless Access Point that can be managed by a FortiGate. Most FortiAP functions can also been accomplished using a FortiWiFi unit.

FortiOS: FortiOS is the operating system used by FortiGate and FortiWiFi units. It is also referred to as firmware.

FTP: File Transfer Protocol is a standard protocol used to transfer computer files from one host to another host over a computer network, usually the Internet, using FTP client and server applications.

Gateway: A gateway is the IP address that traffic is sent to if it needs to reach resources that are not located on the local subnet. In most FortiGate configurations, a default route using a gateway provided by an Internet service provider must be set to allow Internet traffic.

GUI: The Graphical User Interface, also known as the web-based manager, is a graphics-based interface used to configure a FortiGate unit and is an alternative to using the Command Line Interface (see CLI). You can connect to the GUI using either a web browser or FortiExplorer. Most steps in the FortiGate Cookbook use the GUI.

HTTP: Hypertext Transfer Protocol is a protocol used for unencrypted communication over computer networks, including the Internet, where it is used to access websites. FortiGate units handle more HTTP traffic than any other protocol.

HTTPS: Hypertext Transfer Protocol Secure is a protocol that secures HTTP communications using the Secure Sockets Layer (SSL) protocol. HTTPS is the most commonly used secure communication protocol on the Internet.

Interfaces: Interfaces are the points at which communication between two different environments takes place. These points can be physical, like the Ethernet ports on a FortiGate, or logical, like a VPN portal.

IP address: An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. FortiGate units can use IP addresses to filter traffic and determine whether to allow or deny traffic. Both IP version 4 and IP version 6 (see IPv4 and IPv6) are supported by your FortiGate.

IPsec: Internet Protocol Security is used to for securing IP communications by authenticating and encrypting each packet of a session. A FortiGate primarily uses this protocol to secure virtual private networks (see VPN).

IPv4: Internet Protocol version 4 is the fourth version of the Internet Protocol (IP), the main protocol used for communication over the Internet. IPv4 addresses are 32-bit and can be represented in notation by 4 octets of decimal digits, separated by a period: for example, 172.16.254.1.

IPv6: Internet Protocol version 6 is the sixth version of the Internet Protocol (IP), the main protocol used for communication over the Internet (IPv5 never became an official protocol). IPv6 was created

in response to the depletion of available IPv4 addresses. IPv6 addresses are 128-bit and can be represented in notation by 8 octets of hexadecimal digits, separated by a colon: for example, 2001:db8:0000:0000:0000:0000:0000:0000. IPv6 addresses can be shortened if all the octets are 0000; for example, the previous address can also be written as 2001:db8::

LAN/internal: The LAN/internal interface is an interface that some FortiGate models have by default. This interface contains a number of physical ports that are all treated as a single interface by the FortiGate unit. This allows you to configure access for the entire Local Area Network at the same time, rather than configuring each port individually.

LDAP: Lightweight Directory Access Protocol is a protocol used for accessing and maintaining distributed directory information services over a network. LDAP servers are commonly used with a FortiGate for user authentication.

MAC address: A Media Access Control address is a unique identifier assigned to a network interface used for network communication. A MAC address is assigned to a device by the manufacturer and so this address, unlike an IP address, is not normally changed. MAC addresses are represented in notation by six groups of two hexadecimal digits, separated by hyphens or colons: for example, 01:23:45:67:89:ab. Your FortiGate can identify network devices using MAC addresses.

Multicast: Multicast is a method of group communication where information is addressed to a group of destinations simultaneously. A FortiGate can use multicast traffic to allow communication between network devices.

NAT: Network Address Translation is a process used to modify, or translate, either the source or destination IP address or port in a packet header. The primary use for NAT is to allow multiple network devices on a private network to be represented by a single public IP address when they browse the internet. FortiGate also supports many other uses for NAT.

Packet: A packet is a unit of data that is transmitted between communicating devices. A packet contains both the message being sent and control information, such as the source address (the IP address of the device that sent the packet) and the destination address (the IP address of the device the packet is being sent to).

Ping: Ping is a utility used to test whether devices are connected over a IP network and to measure how long it takes for a reply to be received after the message is sent, using a protocol called Internet Control Message Protocol (ICMP). If ICMP is enabled on the destination interface, you can ping the IP address of a FortiGate interface to test connectivity between your computer and the FortiGate. You can also use the CLI command `execute ping` to test connectivity between your FortiGate and both internal and external devices.

Ports: See Interfaces and Port Numbers.

Port numbers: Port numbers are communication endpoints used to allow network communication. Different ports are used for different application-specific or process-specific purposes; for example, HTTP protocol commonly uses port 80.

RADIUS: Remote Authentication Dial In User Service is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service. RADIUS servers are commonly used with a FortiGate for user authentication, including single-sign on.

Session: A session is the dialogue between two or more communicating devices that include all messages that pass between the devices; for example, a session is created when a user browses to a specific website on the Internet for all communication between the user's computer and the web server that hosts the site. Sessions are tracked by a FortiGate unit in order to create logs about the network traffic.

SIP: Session Initiation Protocol is used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol networks. FortiGate units use this protocol for voice over IP (see VoIP).

SNMP: Simple Network Management Protocol is a protocol that monitors hardware on your network. A FortiGate can use SNMP to monitor events such as high CPU usage, VPN tunnels going down, or hardware becoming disconnected.

SSH: Secure Shell is a protocol used for secure network services between two devices, including remote command-line access. SSH can be used to access a FortiGate's command line interface (CLI).

SSID: A Service Set Identifier is the name that a wireless access point broadcasts to wireless users. Wireless users select this name to join a wireless network.

SSL: Secure Sockets Layer is a protocol for encrypting information that is transmitted over a network, including the Internet. SSL can be used for secure communications to a FortiGate, as well as for encrypting Internet traffic (see HTTPS) and for allowing remote users to access a network using SSL virtual private network (see VPN).

SSL inspection: Secure Sockets Layer inspection is used by your FortiGate to scan traffic or communication sessions that use SSL for encryption, including HTTPS protocol.

SSO: Single Sign-On is a feature that allows a user to login just once and remembers the credentials to re-use them automatically if additional authentication is required. A FortiGate supports both Fortinet single sign-on (FSSO) and single sign-on using a RADIUS server (RSSO).

Static route: A static route is a manually-configured routing entry that is fixed and does not change if the network is changed or reconfigured.

Subnet: A subnetwork, or subnet, is a segment of the network that is separated physically by routing network devices and/or logically by the difference in addressing of the nodes of the subnet from other subnets. Dividing the network into subnets helps performance by isolating traffic from segments of the network where it doesn't need to go, and it aids in security by isolating access. The addressing scope of a subnet is defined by its IP address and subnet mask and its connection to other networks is achieve by the use of gateways.

Subnet Mask: A subnet mask is the part of an IP address that is used to determine if two addresses are on the same subnet by allowing any network enabled device, such as a FortiGate, to separate the network address and the host address. This lets the device determine if the traffic needs to be sent through a gateway to an external network or if it is being sent to host on the local network.

VLAN: Virtual Local Area Networks are used to logically divide a single local area network (LAN) into different parts that function independently. A FortiGate uses VLANs to provide different levels of access to users connecting to the same LAN.

VDOM: Virtual Domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

VoIP: Voice over Internet Protocol is a protocol that is used to allow voice communications and multimedia sessions over Internet Protocol sessions, including the Internet. VoIP protocol is used by a FortiGate when traffic needs to reach a connected VoIP phone or FortiVoice unit.

VPN: A Virtual Private Network is a private network that acts as a virtual tunnel across a public network, typically the Internet, and allows remote users to access resources on a private network. There are two main types of VPNs that can be configured using a FortiGate unit: IPsec VPN (see IPsec) and SSL VPN (see SSL).

URL: A Uniform Resource Locator is a text string that refers to a network resource. The most common use for URLs is on the Internet, where they are also known as web addresses. URLs are used by your FortiGate to locate websites on the Internet and can also be used in web filtering to block specific sites from being accessed.

WAN/WAN1: The WAN or WAN1 port on your FortiGate unit is the interface that is most commonly used to connect the FortiGate to a Wide Area Network, typically the Internet. Some FortiGate models have a WAN2 port, which is commonly used for redundant Internet connections.